INTEROPERABILITY OF ELECTRONIC HEALTH RECORDS USING HL7 AND FHIR STANDARDS: A FRAMEWORK FOR INTEGRATED HEALTHCARE SYSTEMS IN SAUDI ARABIA

Abstract

Electronic health records can improve continuity of care only when relevant clinical information follows patients across institutions without losing its meaning, context or security. In Saudi Arabia, the expansion of digital healthcare creates an opportunity to connect hospital information systems, primary care platforms, laboratories, pharmacies, insurers and national exchange services. Yet integration is constrained by legacy interfaces, inconsistent terminologies, patient-matching errors, competing governance arrangements and uneven technical capability. This integrative review examines the contribution of Health Level Seven standards, particularly Fast Healthcare Interoperability Resources, to a practical framework for integrated healthcare systems. It distinguishes transport connectivity from syntactic, semantic, organisational and clinical interoperability, and analyses architecture, implementation guidance, information governance and operational assurance. The proposed framework combines a national governance layer, standardised clinical profiles, terminology services, identity management, secure application programming interfaces, event orchestration and continuous validation. Its contribution is an implementation-oriented model in which interoperability is assessed by whether authorised clinicians receive accurate, timely and usable information, rather than merely by successful message delivery. Saudi institutions can adopt the framework progressively through constrained use cases, transparent measurement, shared conformance testing and strong privacy safeguards.

Keywords

electronic health records; HL7; FHIR; healthcare interoperability; Saudi Arabia; clinical terminology; data governance; health information exchange.

UNDER PEER REVIEW IN IJAR

1: Introduction

Electronic health records have become essential infrastructure for clinical documentation, medication management, diagnostics, referral, discharge and coordinated chronic disease care. The record held by one facility, however, rarely represents the entire experience of a patient. Different providers may maintain separate identifiers, use distinct software suppliers and record similar clinical events with different codes or descriptions. When a receiving clinician cannot locate trustworthy previous results, care may involve avoidable duplication, delayed decisions or incomplete medication reconciliation. Connectivity alone is insufficient: exchanging a file that nobody can reliably interpret does not deliver meaningful interoperability.

Saudi Arabia offers a significant setting for examining these challenges because large public and private networks, specialty hospitals, primary care services and payer systems participate in a rapidly developing digital-health environment. National initiatives encourage integrated services, while clinical organisations must also maintain safety, resilience, confidentiality and business continuity. The national nphies healthcare financial exchange illustrates how specific FHIR implementation rules can coordinate transactions among providers and insurers. Its scope should not be mistaken for proof that every clinical record is already interoperable across the Kingdom.

Health Level Seven International developed several families of exchange standards, including version 2 messaging, Clinical Document Architecture and Fast Healthcare Interoperability Resources. These technologies address different needs and often coexist in the same hospital. HL7 version 2 remains important for laboratory and admission interfaces. Clinical Document Architecture can preserve structured clinical documents. FHIR offers modular resources, defined interfaces and an extensible profiling mechanism that can connect modern applications to existing systems. Effective design requires careful decisions about which information is exchanged, who is allowed to use it and what local adaptations are permissible.

This review investigates how a coherent architecture could translate these standards into reliable information continuity across Saudi settings. It focuses on clinical use cases and the operating conditions necessary to sustain them. The central argument is that standards provide a shared technical language, whereas interoperability emerges from coordinated clinical definitions, identity assurance, governed access, workflow design and quality measurement. A framework that omits any of these components may produce technically valid exchanges that clinicians cannot safely use.

2: Aim Objectives and Research Questions

The aim is to develop a practical standards-based interoperability framework for integrated electronic health record systems in Saudi Arabia, with HL7 and FHIR functioning as complementary technical enablers rather than isolated software products. The proposed model seeks to strengthen patient-centred information continuity while preserving local accountability and national data-protection obligations.

The objectives are to examine barriers across structural, semantic and organisational layers; compare the roles of established HL7 standards and FHIR; specify a modular architecture for clinical exchange; identify governance and cybersecurity safeguards; and formulate a staged implementation and performance-assurance approach suitable for institutions with different levels of digital maturity.

UNDER PEER REVIEW IN IJAR

Four research questions guide the synthesis. What failures prevent records exchanged across Saudi healthcare institutions from being clinically usable? Which combinations of FHIR resources, implementation profiles, clinical terminologies and legacy adapters address these failures? How should identity, consent or other lawful access bases, provenance and security be coordinated across organisations? Which indicators demonstrate improved clinical continuity without overstating the benefits of technical integration? These questions place evidence quality and patient outcomes ahead of technological novelty.

3: Review Methodology

A structured integrative review approach was selected because healthcare interoperability involves clinical informatics, software architecture, governance, security, terminology and health-system operations. The review draws on publicly available technical specifications, implementation guidance, recognised institutional frameworks and relevant scientific literature. Foundational HL7 documentation establishes what a standard actually requires, while implementation guidance and academic research inform its practical use and limitations. The process is a narrative synthesis rather than a registered systematic review or meta-analysis.

Search concepts included electronic health records, HL7 version 2, Clinical Document Architecture, FHIR R4, interoperability, health information exchange, terminology mapping, patient identity, access control, consent, clinical safety, Saudi Arabia and digital health transformation. Relevant information sources include professional and standards organisations, peer-reviewed biomedical informatics outlets and official Saudi digital-health material. Preference was given to sources issued or current during 2020 to 2025, with older foundational specifications retained when indispensable to explaining architecture or terminology.

Evidence was considered for technical relevance, clarity of implementation requirements, direct applicability to clinical exchange and plausibility in Saudi operating conditions. Material was not treated as evidence of improved patient outcomes simply because an interface could pass a technical conformance test. Conversely, context-specific implementation reports were not automatically generalised to every facility. No numerical study-selection totals, pooled effect estimates or exhaustive database-screening claims are made because a reproducible comprehensive screening exercise was not conducted for this manuscript.

The synthesis groups the material into interoperability layers, legacy integration, semantic alignment, architecture, governance, implementation and assurance. A conceptual framework is then derived from common technical and organisational requirements. This method permits a transparent design proposal but cannot establish the measured effectiveness of the framework. Empirical validation in different Saudi clinical settings remains an essential subsequent step.

UNDER PEER REVIEW IN IJAR

4: Interoperability Requirements in Saudi Healthcare

Clinical interoperability operates at several distinct levels. Foundational interoperability permits one system to transmit data to another. Structural interoperability establishes a known format and element organisation. Semantic interoperability preserves the meaning of the information after transfer, including units, codes, timing and clinical context. Organisational interoperability coordinates processes, policies, accountability and incentives among participants. A complete exchange pathway must address all four levels, because failure at one layer can erase progress at the others.

Saudi healthcare networks differ in record systems, clinical workflows, terminology practices, supplier contracts and legacy infrastructure. A national integration programme cannot assume that every hospital can instantly replace existing software or expose the same information model. A realistic framework therefore requires a common minimum exchange contract while allowing local adapters and phased capability development. Shared requirements should define which events initiate exchange, which data items are essential, what level of accuracy is acceptable and how receiving teams handle missing or contradictory information.

Patient identity is a particularly consequential foundation. A technically correct laboratory result linked to the wrong individual may cause direct harm. Matching should use approved identifiers, demographic validation, rules for uncertain matches, controlled exception queues and auditable correction procedures. One identifier should not automatically be treated as globally infallible. Similarly, encounters and clinical episodes need consistent association, especially when patients move between primary care, emergency departments and specialised services.

Saudi institutions must also distinguish national exchange capabilities by their intended use. Financial eligibility, authorisation and claims workflows differ materially from the exchange of longitudinal medication histories or discharge summaries. Reusing underlying standards can reduce duplication, but clinical data should not be repurposed automatically because another platform already transports FHIR messages. Information-sharing decisions must reflect lawful purpose, permitted disclosure, participating organisations and clinical necessity.

5: HL7 Standards and FHIR Capabilities

HL7 version 2 messages remain embedded in hospital operations because they provide established methods for transmitting admissions, discharges, laboratory orders and results. Their flexibility, while historically valuable, can produce local variations that require bilateral interface agreements. Clinical Document Architecture represents documents with structured metadata and optional machine-readable clinical sections, supporting use cases where a complete signed or authored document is the appropriate exchange object. FHIR differs by organising information into smaller resources that can be searched, referenced and assembled for defined purposes.

FHIR resources such as Patient, Encounter, Observation, Condition, AllergyIntolerance, MedicationRequest, DiagnosticReport and CarePlan describe common healthcare concepts. A server can expose interactions using defined web conventions, but deployment decisions must consider privacy, pagination, search restrictions, history, updates and failure behaviour. FHIR is not synonymous with a universal open database: server permissions, supported operations and local profiles determine what a given application may retrieve or submit.

UNDER PEER REVIEW IN IJAR

The version of FHIR matters. Release 4 provides a widely adopted baseline, including mature foundational components, while later releases introduce changes that may not be interchangeable. Integration contracts should state exact package versions and accepted resource profiles. Implementers must not assume that a resource valid under an unconstrained base specification satisfies a Saudi programme's specific rules. Conformance is defined by the applicable implementation guide, not just by well-formed JSON.

FHIR can carry references among clinical concepts and attach provenance, but it does not by itself ensure that the values are meaningful. A vital-sign observation without correct units, time, patient and device context may be unsafe even if syntactically valid. Similarly, a medication code selected from an incompatible catalogue can create apparent equivalence where none exists. Standards should therefore be paired with terminology governance, structured validation and acceptance testing based on clinically realistic scenarios.

6: Semantic Interoperability and Data Quality

Semantic alignment requires deliberate choices about code systems, value sets, local naming conventions and unit conversion. SNOMED CT can represent clinical concepts, LOINC is commonly used for observations and laboratory tests, ICD classifications support defined reporting contexts, and UCUM provides a standard representation for measurement units. Each terminology serves a different purpose; indiscriminate substitution can weaken meaning. An implementation guide should specify mandatory bindings, allowed extensions and procedures for cases where the source system lacks a matching concept.

A central terminology service can support validation, code-system lookups, value-set expansion and mappings between locally used classifications and agreed exchange vocabularies. Such mappings should record their version, effective date, purpose and confidence. Some transformations are approximate rather than exact. When a local term has broader meaning than a target code, a receiving system should not silently treat the two as equivalent. Ambiguity can be represented explicitly and routed for clinical review where consequential.

Quality controls should test completeness, consistency, clinical plausibility, duplication, timeliness and provenance. For example, a potassium result may require both an interpretable unit and specimen context; a medication statement requires attention to status and timing; and an allergy record must distinguish an adverse reaction from an unverified historical label. Validation at an application programming interface boundary should be supplemented by quality monitoring after integration, because records can be schema-valid yet clinically misleading.

Data provenance improves confidence by recording where information originated and whether it was copied, transformed, verified or amended. A longitudinal view should preserve meaningful temporal distinctions rather than flattening all entries into an apparently current problem list. Conflict resolution should not overwrite legitimate differences between sources without accountability. The receiving clinician needs the ability to view origin, timestamp and correction status when an inconsistency could affect decisions.

UNDER PEER REVIEW IN IJAI

Table 1. Interoperability layers and representative validation requirements

Interoperability layer	Principal control	Failure to test
Structural	FHIR profiles and interface contracts	Valid syntax with absent required fields
Semantic	Value sets and terminology mapping	Incorrect units or ambiguous codes
Identity and trust	Patient matching and scoped access	Wrong-patient information access
Clinical workflow	Reconciliation and provenance display	Stale record treated as current

7: Proposed Integrated Interoperability Framework

The proposed framework has seven connected layers. A governance layer establishes accountable stewardship, approved purposes and priorities. An identity and trust layer verifies organisations, users and patients. A connectivity layer incorporates legacy HL7 interfaces, document exchange and FHIR endpoints. A semantic layer manages terminology, profiles and validation. An orchestration layer routes authorised events and queries. A clinical workflow layer presents information in context. An assurance layer evaluates safety, service reliability, privacy and improvement. These layers should be implemented together, even if advanced functions are introduced gradually.

At the system boundary, a hospital integration engine converts supported legacy events into a canonical exchange representation without deleting original messages. A FHIR gateway applies authentication, authorisation, profile validation, rate limits and routing policies. The architecture separates clinical record ownership from exchange services: a shared gateway does not automatically become the definitive source of every clinical fact. Where national exchange infrastructure is used, local systems should conform to the interface and governance requirements of that particular service.

For a discharge scenario, the originating hospital records a finalised summary, medication changes, diagnoses and follow-up arrangements. The integration service verifies identity and transforms source data into agreed resources or documents. The receiving primary care organisation accesses the information only when entitled to do so and sees both clinical content and its provenance. Delivery acknowledgement is distinct from clinical reconciliation; the receiving service remains responsible for reviewing treatment changes and resolving contradictions.

For a laboratory scenario, an order and resulting report must retain patient, encounter, specimen, test identity, result value, unit, reference range, interpretation and status. Messaging and document pathways can coexist with a FHIR access layer, provided transformations are testable and loss is visible. The architecture should support retry, deduplication and exception handling without presenting repeated messages as separate clinical events. Unavailable services should have documented fallback pathways that preserve urgent care.

UNDER PEER REVIEW IN IJAR

The governance layer defines a national minimum dataset and controlled local extensions. This balance permits innovation while maintaining a reliable core. A change-control board including clinicians, informaticians, security specialists and service owners should evaluate new profiles. Technical decisions should be traceable to clinical questions, and each profile should include examples of expected, missing, contradictory and invalid data. Cross-institutional cooperation becomes repeatable when requirements are published and consistently tested.

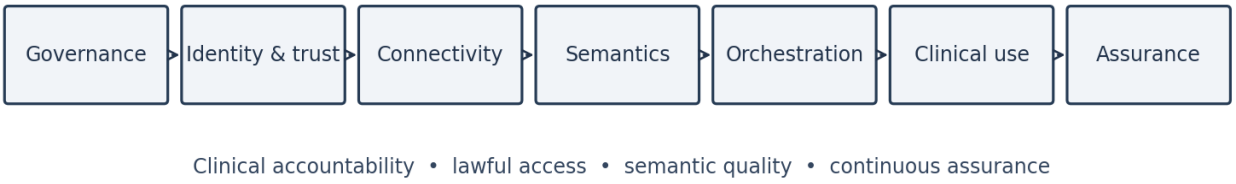


Figure 1. Seven-layer clinical interoperability framework

8: Information Security Privacy and Trust

Interoperability expands the number of systems and users able to access health information, increasing the importance of legal and technical safeguards. Personal health information requires purpose limitation, appropriate collection, minimisation and controlled disclosure under applicable Saudi requirements. An exchange framework should maintain a data inventory, articulate each participating organisation's role and examine any proposed secondary use or cross-border transfer separately. A technical ability to retrieve information does not establish a lawful or clinically appropriate reason to do so.

Authentication should establish the identity of systems and users, while authorisation evaluates whether a particular request is permitted. Role-based access provides a starting point, but context may also matter, including organisation, care relationship, patient, location, purpose and urgency. Emergency access needs explicit conditions, additional logging and retrospective review. Delegated application access must be scoped narrowly enough to prevent a legitimate integration token from becoming unrestricted access to an entire population.

Transport encryption, secure configuration, credential rotation, endpoint monitoring and vulnerability management are necessary but not sufficient. Audit trails should record who accessed which information, when, through which application and under what asserted purpose. Logs must be protected from alteration and should avoid unnecessarily replicating sensitive clinical content. Vendors need clear contractual responsibilities for patching, incident notification, key custody, backups and end-of-service data handling.

FHIR includes security-related resources and conventions, yet practical protection depends on local architecture. A deployment should incorporate threat modelling for misdirected patient matches, compromised interfaces, malicious bulk extraction, excessive API privileges, data poisoning and unavailable terminology services. Downtime procedures must explain which records remain accessible and how clinicians reconcile transactions after recovery. Security controls should preserve safe clinical use rather than create undocumented barriers during emergency care.

UNDER PEER REVIEW

9: Implementation Roadmap and Conformance Assurance

Implementation should begin with a small number of clinically valuable exchange pathways rather than an ambition to expose every database table immediately. Suitable candidates include discharge summaries, medication reconciliation, laboratory result availability and structured referrals. Each pathway needs a named clinical owner, participating organisations, minimum dataset, legal basis, expected workload and baseline performance measures. The business case should identify a specific care problem and explain how better information access could address it.

The first phase is readiness assessment. Participating organisations inventory existing HL7 messages, documents, database interfaces, coding practices and vendor contracts. They identify source-of-truth systems, record-quality problems, operational dependencies and integration skills. The second phase establishes agreed profiles, terminology bindings, test cases, identity controls and escalation procedures. The third builds and tests adapters in a controlled environment using realistic synthetic or appropriately protected datasets.

Technical conformance testing should verify resource structure, required elements, cardinality, terminology bindings, identifiers and declared server capabilities. Scenario testing should examine duplicate messages, missing units, conflicting demographics, inaccessible services, delayed updates and patient-merging events. Security testing should include attempts to access another patient's records, overbroad searches and invalid authorisation scopes. Clinicians should participate in acceptance tests because software teams may not recognise harmful misinterpretations that satisfy a schema.

A supervised pilot should monitor both system behaviour and clinical usability. Participants should record how often available information is incorporated into care and when staff must telephone another facility to clarify it. Before scaling, the steering group should review failures, exception backlogs, staff feedback, security events and operating cost. Wider rollout should follow common onboarding criteria and a documented rollback mechanism. Success is a sustained capability to exchange and use information safely, not a one-time demonstration of a successful API call.

Table 2. Measures for clinical interoperability assurance

Assessment domain	Example measure	Interpretation
Technical conformance	Percentage of transactions passing profile tests	Checks conformity, not clinical value
Semantic accuracy	Clinician-reviewed mapping error rate	Tests preservation of clinical meaning
Identity safety	Incorrect patient-linkage events	Tracks high-severity matching failures
Operational usability	Time to obtain clinically usable summary	Tests real workflow improvement

UNDER PEER REVIEW IN IJAR

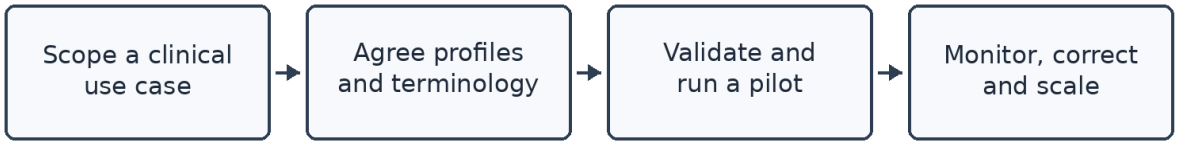


Figure 2. Controlled implementation and scaling pathway

10: Discussion

The analysis indicates that HL7 and FHIR can provide the technical foundation for Saudi healthcare integration, but the most difficult barriers are not purely technical. Organisations may share a FHIR version and still disagree about medication status, episode boundaries or responsibility for correcting an inaccurate result. Standardisation must therefore operate simultaneously at the level of data definitions, institutional relationships and clinical workflow. The framework places governance and assurance alongside connectivity to prevent integration projects from becoming isolated interface-building exercises.

One practical advantage of FHIR is its modularity. Teams can publish clearly bounded information services without forcing a single replacement electronic health record across every provider. This is valuable in heterogeneous markets, but modularity also introduces complexity. Different applications may request overlapping resource collections, construct different longitudinal views and interpret the absence of information inconsistently. Programme-level profiles, searchable capability statements and representative test cases are needed to make modular interfaces predictable.

Legacy systems should be treated as continuing participants rather than temporary obstacles. Large hospitals may depend on stable HL7 version 2 feeds for real-time operations. A poorly designed conversion layer can lose event order, introduce duplicate encounters or mislabel observations. Integration programmes should preserve source messages for reconciliation, use idempotent processing where practical and implement observable error queues. Replacement can occur where justified, but a coexistence strategy reduces implementation risk and makes investment more manageable.

Clinical safety provides the decisive evaluative perspective. A resource may arrive within seconds and still mislead clinicians if it refers to an obsolete prescription or if a critical allergy was omitted. Therefore, measurement should include semantic correctness and whether recipients can identify provenance and uncertainty. Test suites should pair machine-readable checks with clinician assessment of realistic records. Adverse-event reporting and near-miss review should be able to identify defects introduced by mapping, identity resolution or presentation layers.

An implementation programme should also plan the practical stewardship of shared implementation artefacts. Every approved profile needs an accessible specification, version history, sample payloads, identified maintainers, and an effective date. Training environments should be stable enough for suppliers to reproduce failures and verify fixes. Clinicians need a straightforward way to raise concerns when a mandatory field is inadequate for a real care scenario. A formal

UNDER PEER REVIEW IN IJAR

change request should capture the clinical justification, impact on existing interfaces, compatibility implications and migration period. Without this operational discipline, standards can fragment through undocumented local patches even when participants originally adopted a common specification.

The proposed framework also highlights a tension between national consistency and local flexibility. Too much local variation fragments exchange; excessively rigid rules may exclude specialist workflows or burden smaller providers. A stable core profile with a governed extension process offers a defensible compromise. Every extension should have a clear purpose and should not change the meaning of mandatory core fields. Publicly available guidance and version control can reduce bilateral negotiation and support supplier accountability.

Another tension concerns information availability and confidentiality. Broad access may reduce delays yet also increase exposure if service relationships and authorisation are not evaluated. Overly restrictive access can undermine continuity during referrals and emergencies. A proportional design combines robust identity checks, transparent permissions, context-sensitive controls and auditable exceptions. The answer cannot be a single universal access setting. Institutions must coordinate clinical duties, patient rights and applicable national rules.

Data governance is especially challenging when records are copied into multiple repositories. Correction of an erroneous diagnosis at the source may not propagate automatically, leaving inconsistent views. The framework recommends version-aware exchange, provenance retention, correction events and reconciliation responsibilities. Clinicians should distinguish information that was observed directly from material imported from another provider. A national patient summary can improve access, but only if its assembly, update frequency and completeness are clearly explained.

Terminology services offer economies of scale, yet local clinical validation remains essential. A laboratory mapping may be technically well formed while relating tests with different specimens or methods. Pharmacy mappings can obscure formulation or strength differences. National code lists should be governed by appropriate domain experts, with transparent release cycles and test environments. Semantic quality requires a continuous stewardship programme, not a one-off translation project.

Procurement and vendor incentives can also shape interoperability. Suppliers may implement minimum compliance while charging heavily for additional interfaces or limiting access to export functions. Contracts should clarify standards conformance, version support, documentation rights, data portability, incident response and exit provisions. Buyers should evaluate whether interoperability functions work against independent test systems rather than accepting promotional claims. Conformance evidence should be repeatable after software upgrades.

The national context introduces further operational considerations. Rural facilities, smaller clinics and mobile services may have variable connectivity, infrastructure and specialist capacity. An integration framework needs graceful degradation, queued exchange where suitable and escalation when information is delayed. Emergency workflows cannot depend entirely on an always-available remote endpoint. Organisations must provide safe alternatives and reconcile locally captured information once services return.

Healthcare staff experience should shape interface design. A technically comprehensive record can overwhelm a practitioner when key changes are buried among duplicated observations. Applications should prioritise clinically relevant summaries, preserve detail on demand and clearly

UNDER PEER REVIEW IN IJAP

identify source and currency. Alert fatigue can arise from incorrect allergy, interaction or overdue-test flags imported from incomplete records. Usability testing should assess whether integrated information improves decisions rather than merely increasing visible data volume.

The framework is a conceptual proposal, not evidence that a specific deployment has reduced mortality, costs or diagnostic error. Such outcomes depend on case mix, adoption, quality of source records and organisational practices. Stronger evaluation will require prospective comparison, suitable control groups or carefully designed time-series studies. Metrics should include both benefits and unintended consequences, including staff workload, delayed care caused by outages and privacy incidents. This balanced evaluation is necessary for responsible national scaling.

11: Research Gaps and Future Research

Several gaps require investigation in Saudi settings. First, comparative studies should measure semantic accuracy across common EHR vendors and settings rather than report only successful transaction counts. Second, research should assess patient identity matching across facilities with different documentation practices, including rates of false linkage and unresolved duplicates. Third, longitudinal studies are needed to determine whether interoperable medication histories and discharge summaries change reconciliation quality, avoidable testing or referral delays.

Additional work should investigate the performance and cost of terminology services in bilingual clinical environments, including local abbreviations and inconsistent translation. Studies should examine whether governance templates and standard implementation guides reduce supplier-specific customisation, and how smaller providers can meet conformance requirements without disproportionate expense. Security research should test realistic threat scenarios involving API misuse, emergency access, third-party applications and exchanged data retained outside the originating institution.

Future evaluations should publish detailed interface versions, profile packages, denominators and failure definitions. Prospective implementation research can compare phased rollout sites against appropriate baselines while accounting for clinical workload and digital maturity. Patient and clinician perspectives deserve direct study because technical adoption may not represent meaningful access or trust. Finally, researchers should explore how to coordinate data-quality correction across interconnected providers while keeping clear responsibility for original records.

12: Practical Managerial and Policy Implications

Hospital executives should treat interoperability as a clinical service improvement programme with technical components, not as an infrastructure purchase. Clinical leaders should define priority exchanges and acceptance criteria; information technology teams should manage integration, availability and performance; informatics specialists should own clinical concepts and mapping; privacy and cybersecurity officers should establish safe access boundaries. Each use case needs an accountable owner capable of resolving cross-departmental disputes.

Managers should fund continuous terminology stewardship, profile maintenance, vendor regression testing and staff training after initial deployment. Budgets focused only on API development underestimate the effort required to maintain trustworthy information. Procurement should demand conformance evidence, transparent documentation, controlled upgrades and data-export capability. Providers should report both interoperability failures and successful recoveries to support learning across organisations.

UNDER PEER REVIEW IN IJAR

Policy makers and sector bodies can encourage a stable minimum clinical dataset, common conformance tests and transparent versioned implementation guidance. Collaboration forums should include hospitals, primary care, pharmacies, laboratories, software vendors and patient representatives. Guidance should define safeguards for clinical access, patient identity, correction and emergency circumstances without prescribing one vendor architecture. National progress should be measured through safe clinical information use rather than raw counts of connected interfaces.

13: Limitations

This manuscript is an integrative conceptual review and does not report original interviews, experiments, direct access to Saudi clinical datasets or a systematic screening count. Public specifications establish interface requirements but cannot independently demonstrate local conformance or clinical impact. The framework is sensitive to changes in FHIR releases, national implementation guidance, governance arrangements and security requirements. Differences in provider maturity and speciality may limit transferability. Actual deployment requires clinical safety assessment, legal review, vendor testing and prospective evaluation.

14: Conclusion

HL7 standards and FHIR can support an integrated Saudi electronic health record ecosystem when their technical capabilities are combined with semantic consistency, reliable identity management, appropriate security and accountable clinical workflows. The proposed seven-layer framework links governance, trust, connectivity, terminology, orchestration, clinical use and assurance. It recognises the continuing role of legacy systems while providing a path toward governed modern interfaces. Priority should be given to carefully selected exchange scenarios, explicit implementation profiles, clinician-led validation and objective measurement of usability and safety. Genuine interoperability is achieved not when two systems exchange structured data, but when a receiving professional can use accurate, timely and appropriately authorised information to provide better coordinated care.

UNDER PEER REVIEW IN IJAR

References

[1] HL7 International. (2019). FHIR Release 4 (version 4.0.1): Specification. https://hl7.org/fhir/R4/

[2] HL7 International. (2023). FHIR Release 5: Specification. https://hl7.org/fhir/R5/

[3] HL7 International. (2019). FHIR R4 RESTful API. https://hl7.org/fhir/R4/http.html

[4] HL7 International. (2019). FHIR R4 Profiling. https://hl7.org/fhir/R4/profiling.html

[5] HL7 International. (2019). FHIR R4 Terminology Service. https://hl7.org/fhir/R4/terminology-service.html

[6] HL7 International. (2019). FHIR R4 Security and Privacy. https://hl7.org/fhir/R4/secpriv-module.html

[7] HL7 International. (2019). FHIR R4 Provenance Resource. https://hl7.org/fhir/R4/provenance.html

[8] HL7 International. (2019). FHIR R4 AuditEvent Resource. https://hl7.org/fhir/R4/auditevent.html

[9] HL7 International. (2019). FHIR R4 Consent Resource. https://hl7.org/fhir/R4/consent.html

[10] HL7 International. (2019). FHIR R4 CapabilityStatement Resource. https://hl7.org/fhir/R4/capabilitystatement.html

[11] HL7 International. (2019). FHIR R4 StructureDefinition Resource. https://hl7.org/fhir/R4/structuredefinition.html

[12] HL7 International. (2019). FHIR R4 Bundle Resource. https://hl7.org/fhir/R4/bundle.html

[13] HL7 International. (2019). FHIR R4 Patient Resource. https://hl7.org/fhir/R4/patient.html

[14] HL7 International. (2019). FHIR R4 Observation Resource. https://hl7.org/fhir/R4/observation.html

[15] HL7 International. (2019). FHIR R4 DiagnosticReport Resource. https://hl7.org/fhir/R4/diagnosticreport.html

[16] HL7 International. (2019). FHIR R4 MedicationRequest Resource. https://hl7.org/fhir/R4/medicationrequest.html

[17] HL7 International. (2019). FHIR R4 AllergyIntolerance Resource. https://hl7.org/fhir/R4/allergyintolerance.html

[18] HL7 International. (2019). FHIR R4 DocumentReference Resource. https://hl7.org/fhir/R4/documentreference.html

[19] HL7 International. (2019). FHIR R4 ImplementationGuide Resource. https://hl7.org/fhir/R4/implementationguide.html

[20] HL7 International. (2019). FHIR R4 SMART App Launch Framework references and specifications overview. https://hl7.org/fhir/R4/smart-app-launch.html

[21] Council of Health Insurance. (2025). nphies Healthcare Financial Services Implementation Guide: Technical overview. https://portal.nphies.sa/ig/

[22] Council of Health Insurance. (2022). nphies national platform: Integration and implementation information. https://chi.gov.sa/en/Uniplat/Pages/default3.aspx

UNDER PEER REVIEW IN IJAR

[23] Council of Health Insurance. (2026). Payers Qualification and Classification Program: Healthcare information management requirements. https://www.chi.gov.sa/aboutchi/CCHIprograms/DocLib/CHI%E2%80%99s%20Payers%E2%80%99%20Qualification%20and%20Classification%20Program.pdf

[24] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems.

[25] Kingdom of Saudi Arabia. (2021). Personal Data Protection Law, Royal Decree No. M/19 (as amended).

UNDER PEER REVIEW IN IJAR